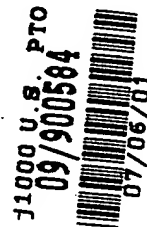


日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application:

2000年 7月 6日

出願番号
Application Number:

特願2000-205615

出願人
Applicant(s):

ソニー株式会社

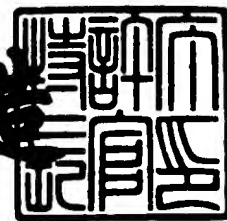
#4
1-25-02

CERTIFIED COPY OF
PRIORITY DOCUMENT

2001年 5月25日

特許庁長官
Commissioner,
Japan Patent Office

及川耕造



出証番号 出証特2001-3044713

【書類名】 特許願

【整理番号】 0000611406

【提出日】 平成12年 7月 6日

【あて先】 特許庁長官殿

【国際特許分類】 G06F 9/00

【発明者】

 【住所又は居所】 東京都品川区北品川6丁目7番35号 ソニー株式会社
内

 【氏名】 中野 雄彦

【特許出願人】

 【識別番号】 000002185

 【氏名又は名称】 ソニー株式会社

 【代表者】 出井 伸之

【代理人】

 【識別番号】 100082131

 【弁理士】

 【氏名又は名称】 稲本 義雄

 【電話番号】 03-3369-6479

【手数料の表示】

 【予納台帳番号】 032089

 【納付金額】 21,000円

【提出物件の目録】

 【物件名】 明細書 1

 【物件名】 図面 1

 【物件名】 要約書 1

 【包括委任状番号】 9708842

【ブルーフの要否】 要

【書類名】 明細書

【発明の名称】 情報処理装置および方法、並びに記録媒体

【特許請求の範囲】

【請求項 1】 ネットワークを介して他の装置にコンテンツを送信する情報処理装置において、

前記コンテンツを暗号化する暗号化手段と、

前記他の装置より受信許可が要求された場合、前記他の装置と認証する認証手段と、

前記認証手段の認証結果に基づいて、前記コンテンツの暗号を解除する解除鍵とともに、受信台数を制限する制限情報を前記他の装置に送信する送信手段とを備えることを特徴とする情報処理装置。

【請求項 2】 前記認証手段の認証結果に基づいて、前記他の装置の識別情報を取得する取得手段と、

前記取得手段により取得された前記識別情報に基づいて、前記受信台数を計数する計数手段と、

前記計数手段により計数された前記識別情報を記憶する記憶手段と

をさらに備えることを特徴とする請求項 1 に記載の情報処理装置。

【請求項 3】 前記送信手段により前記他の装置に前記解除鍵および前記制限情報が送信された場合、または、前記解除鍵が変更された場合、前記制限情報を更新する更新手段をさらに備える

ことを特徴とする請求項 1 に記載の情報処理装置。

【請求項 4】 ネットワークを介して他の装置にコンテンツを送信する情報処理装置の情報処理方法において、

前記コンテンツを暗号化する暗号化ステップと、

前記他の装置より受信許可が要求された場合、前記他の装置と認証する認証ステップと、

前記認証ステップの処理による認証結果に基づいて、前記コンテンツの暗号を解除する解除鍵とともに、受信台数を制限する制限情報を前記他の装置に送信する送信ステップと

を含むことを特徴とする情報処理方法。

【請求項 5】 ネットワークを介して他の装置にコンテンツを送信する情報処理装置用のプログラムにおいて、

前記コンテンツを暗号化する暗号化ステップと、

前記他の装置より受信許可が要求された場合、前記他の装置と認証する認証ステップと、

前記認証ステップの処理による認証結果に基づいて、前記コンテンツの暗号を解除する解除鍵とともに、受信台数を制限する制限情報を前記他の装置に送信する送信ステップと

を含むことを特徴とするコンピュータが読み取り可能なプログラムが記録されている記録媒体。

【請求項 6】 ネットワークを介して他の情報処理装置からコンテンツを受信する情報処理装置において、

前記他の情報処理装置に対して、受信許可の要求を送信する第 1 の送信手段と

、
前記受信許可の要求を送信したとき、前記コンテンツの暗号を解除する解除鍵とともに受信台数を制限する制限情報を、前記他の情報処理装置から受信する受信手段と、

前記受信手段により受信された前記解除鍵に基づいて、前記コンテンツを復号した後、暗号化する暗号化手段と、

前記受信手段により受信された前記制御情報に基づいて、前記暗号化手段により暗号化された前記コンテンツを他の装置に出力する出力手段と

を備えることを特徴とする情報処理装置。

【請求項 7】 ネットワークを介して他の情報処理装置からコンテンツを受信する情報処理装置の情報処理方法において、

前記他の情報処理装置に対して、受信許可の要求を送信する送信ステップと、

前記受信許可の要求を送信したとき、前記コンテンツの暗号を解除する解除鍵とともに受信台数を制限する制限情報を、前記他の情報処理装置から受信する受信ステップと、

前記受信ステップの処理により受信された前記解除鍵に基づいて、前記コンテンツを復号した後、暗号化する暗号化ステップと、

前記受信ステップの処理により受信された前記制御情報に基づいて、前記暗号化ステップの処理により暗号化された前記コンテンツを他の装置に出力する出力ステップと

を含むことを特徴とする情報処理方法。

【請求項 8】 ネットワークを介して他の情報処理装置からコンテンツを受信する情報処理装置用のプログラムにおいて、

前記他の情報処理装置に対して、受信許可の要求を送信する送信ステップと、

前記受信許可の要求を送信したとき、前記コンテンツの暗号を解除する解除鍵とともに受信台数を制限する制限情報を、前記他の情報処理装置から受信する受信ステップと、

前記受信ステップの処理により受信された前記解除鍵に基づいて、前記コンテンツを復号した後、暗号化する暗号化ステップと、

前記受信ステップの処理により受信された前記制御情報に基づいて、前記暗号化ステップの処理により暗号化された前記コンテンツを他の装置に出力する出力ステップと

を含むことを特徴とするコンピュータが読み取り可能なプログラムが記録されている記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、情報処理装置および方法、並びに記録媒体に関し、特に、コンテンツの利用を制限することができるようにした情報処理装置および方法、並びに記録媒体に関する。

【0002】

【従来の技術】

近年、インターネットに代表されるネットワークシステムが普及してきた。これにより、ユーザは、インターネットを介して情報を発信したり、あるいは、情

報を受け取ったりすることができる。

【0003】

【発明が解決しようとする課題】

ところで、映画や音楽などの著作物の視聴を希望する利用者は、それに対する対価を支払うことにより、その著作物を受け取ることができる。

【0004】

しかしながら、インターネットなどのネットワークを通じて、映画や音楽などの著作物が、その所有者だけでなく、著作物に対する対価を支払っていない多くの利用者に対して、不正に視聴されてしまう恐れがあった。

【0005】

また、ネットワークを通じて不正に視聴される行為が無制限に行われるようになると、コンテンツ作成および流通ビジネスを阻害する恐れがあった。

【0006】

本発明はこのような状況に鑑みてなされたものであり、コンテンツが、ネットワークを介して、不正に利用されるのを防止することができるようにするものである。

【0007】

【課題を解決するための手段】

本発明の第1の情報処理装置は、コンテンツを暗号化する暗号化手段と、他の装置より受信許可が要求された場合、他の装置と認証する認証手段と、認証手段の認証結果に基づいて、コンテンツの暗号を解除する解除鍵とともに、受信台数を制限する制限情報を他の装置に送信する送信手段とを備えることを特徴とする。

【0008】

本発明の第1の情報処理装置は、認証手段の認証結果に基づいて、他の装置の識別情報を取得する取得手段と、取得手段により取得された識別情報に基づいて、受信台数を計数する計数手段と、計数手段により計数された識別情報を記憶する記憶手段とをさらに設けるようにすることができる。

【0009】

本発明の第 1 の情報処理装置は、送信手段により他の装置に解除鍵および制限情報が送信された場合、または、解除鍵が変更された場合、制限情報を更新する更新手段をさらに設けるようにすることができる。

【 0 0 1 0 】

本発明の第 1 の情報処理方法は、コンテンツを暗号化する暗号化ステップと、他の装置より受信許可が要求された場合、他の装置と認証する認証ステップと、認証ステップの処理による認証結果に基づいて、コンテンツの暗号を解除する解除鍵とともに、受信台数を制限する制限情報を他の装置に送信する送信ステップとを含むことを特徴とする。

【 0 0 1 1 】

本発明の第 1 の記録媒体に記録されているプログラムは、コンテンツを暗号化する暗号化ステップと、他の装置より受信許可が要求された場合、他の装置と認証する認証ステップと、認証ステップの処理による認証結果に基づいて、コンテンツの暗号を解除する解除鍵とともに、受信台数を制限する制限情報を他の装置に送信する送信ステップとを含むことを特徴とする。

【 0 0 1 2 】

本発明の第 1 の情報処理装置、第 1 の情報処理方法、および第 1 の記録媒体に記録されているプログラムにおいては、コンテンツが暗号化され、他の装置より受信許可が要求された場合、他の装置と認証され、その認証結果に基づいて、コンテンツの暗号を解除する解除鍵とともに、受信台数を制限する制限情報が他の装置に送信される。

【 0 0 1 3 】

本発明の第 2 の情報処理装置は、他の情報処理装置に対して、受信許可の要求を送信する第 1 の送信手段と、受信許可の要求を送信したとき、コンテンツの暗号を解除する解除鍵とともに受信台数を制限する制限情報を、他の情報処理装置から受信する受信手段と、受信手段により受信された解除鍵に基づいて、コンテンツを復号した後、暗号化する暗号化手段と、受信手段により受信された制御情報に基づいて、暗号化手段により暗号化されたコンテンツを他の装置に出力する出力手段とを備えることを特徴とする。

【 0 0 1 4 】

本発明の第2の情報処理方法は、他の情報処理装置に対して、受信許可の要求を送信する送信ステップと、受信許可の要求を送信したとき、コンテンツの暗号を解除する解除鍵とともに受信台数を制限する制限情報を、他の情報処理装置から受信する受信ステップと、受信ステップの処理により受信された解除鍵に基づいて、コンテンツを復号した後、暗号化する暗号化ステップと、受信ステップの処理により受信された制御情報に基づいて、暗号化ステップの処理により暗号化されたコンテンツを他の装置に出力する出力ステップとを含むことを特徴とする。

【 0 0 1 5 】

本発明の第2の記録媒体に記録されているプログラムは、他の情報処理装置に対して、受信許可の要求を送信する送信ステップと、受信許可の要求を送信したとき、コンテンツの暗号を解除する解除鍵とともに受信台数を制限する制限情報を、他の情報処理装置から受信する受信ステップと、受信ステップの処理により受信された解除鍵に基づいて、コンテンツを復号した後、暗号化する暗号化ステップと、受信ステップの処理により受信された制御情報に基づいて、暗号化ステップの処理により暗号化されたコンテンツを他の装置に出力する出力ステップとを含むことを特徴とする。

【 0 0 1 6 】

本発明の第2の情報処理装置、第2の情報処理方法、および第2の記録媒体に記録されているプログラムにおいては、他の情報処理装置に対して、受信許可の要求を送信したとき、コンテンツの暗号を解除する解除鍵とともに受信台数を制限する制限情報が受信され、受信された解除鍵に基づいて、コンテンツが復号された後、暗号化される。そして、受信された制御情報に基づいて、暗号化されたコンテンツが他の装置に出力される。

【 0 0 1 7 】

【発明の実施の形態】

図1は、本発明を適用したネットワークシステムの構成例を示すブロック図である。このネットワークシステムにおいては、ソース1が、バス4-1を介して

、シンク 2-1 およびブリッジ 3-1 に接続され、また、ブリッジ 3-1 が、バス 4-2 を介して、シンク 2-2 およびブリッジ 3-2 に接続され、さらに、ブリッジ 3-2 が、バス 4-3 を介して、シンク 2-3, 2-4 に接続されている。

【0018】

ソース 1 は、コンテンツを出力する出力装置である。コンテンツを出力する場合、ソース 1 は、コンテンツを暗号化した後、バス 4-1 乃至 4-3 を介して、シンク 2-1 乃至 2-4 に出力する。なお、暗号化されたコンテンツの復号に必要な鍵情報は、認証処理に成功したシンクにだけ渡される。これにより、コンテンツを受信するシンクの台数が制限される。なお、後述するブリッジ 3-1, 3-2 は、受信した信号を再出力するだけなので、台数カウントの対象から除外される。

【0019】

シンク 2-1 乃至 2-4 (以下、シンク 2-1 乃至 2-4 を個々に区別する必要がある場合、単にシンク 2 と記載する。その他の装置においても同様とする) は、ソース 1 より供給されたコンテンツを受信する受信装置である。認証処理に成功した場合、シンク 2 は、ソース 1 より渡された鍵情報に基づいて、受信したコンテンツを復号する。

【0020】

ブリッジ 3-1, 3-2 は、ソース 1 より出力された、暗号化されているコンテンツを受信し、復号した後、再び暗号化してシンク 2-2 乃至 2-4 に出力する。そのため、ブリッジ 3 は、ソース 1 と認証処理を行い、暗号化されたコンテンツの復号に必要な鍵情報を取得するとともに、再出力するコンテンツを何台のシンク 2 に受信させたいか否かの制限情報も取得する。すなわち、ブリッジ 3 は、ソース 1 に代わって、コンテンツを受信するシンク 2 の台数を制限する。

【0021】

図 2 は、ソース 1 の詳細な構成例を示すブロック図である。

【0022】

コンテンツプレーヤ 11 は、メディア 12 が装着されると、制御部 15 の制御

に基づいて、メディア 1 2 に記録されているコンテンツを再生し、暗号部 1 3 に出力する。暗号部 1 3 は、コンテンツプレーヤ 1 1 より入力されたコンテンツを暗号化し、通信 I/F (インタフェース) 1 4 を介して、外部に出力する。

【 0 0 2 3 】

制御部 1 5 は、コンテンツプレーヤ 1 2、暗号部 1 3、通信 I/F 1 4、および記憶部 1 6 を制御する。制御部 1 5 はまた、コンテンツプレーヤ 1 1 で再生されたコンテンツを、必要に応じて、記憶部 1 6 に記憶させる。

【 0 0 2 4 】

図 3 は、シンク 2 の詳細な構成例を示すブロック図である。

【 0 0 2 5 】

制御部 2 4 は、画像・音声出力部 2 1、復号部 2 2、通信 I/F 2 3、および、記憶部 2 5 を制御する。制御部 2 4 はまた、通信 I/F 2 3 を介して送信されてきた、暗号化されているコンテンツを記憶部 2 5 に記憶させる。

【 0 0 2 6 】

復号部 2 2 は、通信 I/F 2 3 を介してソース 1 より送信されてきた鍵情報を取得する。復号部 2 2 はまた、記憶部 2 5 に記憶されているコンテンツを、取得した鍵情報に基づいて復号する。画像・音声出力部 2 1 は、復号部 2 2 で復号されたコンテンツを出力する。

【 0 0 2 7 】

図 4 は、ブリッジ 3 の詳細な構成例を示すブロック図である。

【 0 0 2 8 】

制御部 3 5 は、通信 I/F 3 1、復号部 3 2、暗号部 3 3、通信 I/F 3 4、および、記憶部 3 6 を制御する。制御部 3 5 はまた、通信 I/F 3 1 を介して送信されてきた、暗号化されているコンテンツを記憶部 3 6 に記憶させる。

【 0 0 2 9 】

復号部 3 2 は、通信 I/F 3 1 を介してソース 1 より送信されてきた鍵情報を取得するとともに、再出力するコンテンツを何台のシンク 2 に受信させるか否かの制限情報も取得する。復号部 3 2 はまた、記憶部 3 6 に記憶されているコンテンツを、取得した鍵情報と制限情報に基づいて復号する。

【 0 0 3 0 】

暗号部 3 3 は、復号部 3 2 で復号されたコンテンツを暗号化し、通信 I/F 3 4 を介して、外部に出力する。

【 0 0 3 1 】

なお、認証には、公開鍵暗号技術を用いるものとし、ソース 1、シンク 2、およびブリッジ 3 は鍵管理組織が発行する各機器用の Digital Certificate（以下、Certificate と記載する）と各機器用の秘密鍵と鍵管理組織の公開鍵を持つものとする。この Certificate には各機器用の秘密鍵と対応する各機器用の公開鍵、その機器の固有 ID、そしてこの 2 つのデータに対する鍵管理組織による電子署名が含まれるものとする。

【 0 0 3 2 】

図 5 は、ソース 1 とシンク 2 - 1（図 1）が、直接接続される場合の認証処理を説明する図である。

【 0 0 3 3 】

まず、シンク 1 が自分の Certificate をソース 2 - 1 に送信する。具体的には、シンク 1 の制御部 1 5 が、記憶部 1 6 から Certificate を読み出し、通信 I/F 1 4 を介して、ソース 2 - 1 に通信コマンドとして送信する（図 5 ①）。

【 0 0 3 4 】

ソース 2 は、この通信コマンドを受信すると、そのデータが正当なものか否かを判定する。具体的には、ソース 2 - 1 の制御部 2 4 が、記憶部 2 5 に記憶されている鍵管理組織の公開鍵を用いて、通信 I/F 2 3 を介して受信した Certificate 中のデータと、それらに付随する鍵管理組織の電子署名が対応しているのか否かを調べる。すなわち、制御部 2 4 は、公開鍵暗号の DSA (Digital Signature Algorithm) Verify 演算処理を実行することにより、受信データの正当性を判定する。そして、判定結果が、正当である場合、認証処理を継続し、そうでない場合、認証処理を終了する。

【 0 0 3 5 】

処理を継続する場合、ソース 1 の制御部 1 5 は、Certificate 中の相手の ID が記憶部 1 6 に保持する認証済み ID リスト（以下、ID リストと記載する）に登録済

みであるか否かを調べ、登録済みの場合、変数CntUpに0を代入する。

【0036】

一方、IDリストにCertificate中の相手のIDが未登録の場合、ソース1の制御部15は、受信を許可したシンク2の数（以下、変数SinkCntと記載する）と受信を許可できる上限数（以下、変数MaxSinkと記載する）を比較し、変数SinkCntの方が小さければ変数CntUpに1を代入する。

【0037】

なお、SinkCnt=MaxSinkの場合、認証処理は終了される。また、変数MaxSinkは、変数でなくてもよい（すなわち、定数であってもよい）。

【0038】

そして、ソース1の制御部15は、擬似乱数生成アルゴリズムにより、擬似乱数Random_challengeを生成し、シンク2に通信コマンドとして送信する（図5②）。

【0039】

シンク2-1の制御部24は、この通信コマンドを受信すると、その値に対して、記憶部25に保持されている自分自身の秘密鍵を用いて、公開鍵暗号のDSA Sign演算処理を実行して、電子署名を計算する。シンク2-1の制御部24は、計算された電子署名を、通信コマンド（Responseデータ）として、ソース1に送信する（図5③）。

【0040】

ソース1の制御部15は、この通信コマンドを受信すると、自分が送った擬似乱数Random_challengeとこの電子署名が対応しているか否か、すなわち、上述したDSA Verify演算処理を実行して、データの正当性を判定する。ただし、ここでは、先の鍵管理組織の公開鍵の代わりに、相手から受け取ったCertificate中の相手の公開鍵が用いられる。そして、判定結果が、正当である場合、認証処理が継続され、そうでない場合、認証処理は終了される。

【0041】

処理を継続する場合、ソース1の制御部15は、コンテンツにかけた暗号を解くのに必要な鍵情報をシンク2-1に通信コマンドとして送信し（図5④）、変

数SinkCntの値を変数CntUpの値だけ増加する。そして、ソース1の制御部15は、Certificate中の相手のIDが記憶部16に保持する認証済みIDリストに登録済みであるか否かを調べ、登録済みの場合、変数CntUpに0を代入する。一方、IDリストにCertificate中の相手のIDが未登録の場合、変数SinkCntと変数MaxSinkを比較し、変数SinkCntの方が小さければ変数CntUpに1を代入する。

【0042】

シンク2-1は、鍵情報を受信し、それを使ってコンテンツにかけられた暗号を解くことによって、コンテンツを受信することができる。

【0043】

また、図1に示されるソース1とシンク2-2のように、ソース1より出力されたコンテンツが、ブリッジ3-1を経由した後に、シンク2-2に受信される場合、やはり、シンク2-2とブリッジ3-1は、図5に示されたような認証処理を行う。すなわち、ソース1とシンク2-3、または、ソース1とシンク2-4のように、2台以上のブリッジ経由でコンテンツが伝送される場合でも、シンク1と最後のブリッジ3-2（シンク2-3、2-4と直接つながるブリッジ）は同様の認証処理を行う。

【0044】

以上の認証処理におけるシンク2の処理フローを図6に、ソース1の処理フローを図7に、それぞれ示す。

【0045】

シンク1の認証処理は、相手がブリッジ3であっても、ソース2の場合と全く同じである。ブリッジ3の認証処理は、図7のステップS15に示す処理が、ソース2の場合と異なる。具体的には、SinkCnt=MaxSinkの場合、ブリッジ3は、変数MaxSinkの値を大きくするために、自分自身が受信（入力）しているコンテンツの発信元であるソース1またはブリッジ3（図1の例の場合、ブリッジ3-1ならソース1、ブリッジ3-2ならブリッジ3-1）に受信許可を要求する認証処理を行う。なお、この場合には、1台以上の受信台数の追加が要求される。この認証処理が成功した場合、図7のステップS16以降の処理が継続される。

【0046】

図8は、ソース1とブリッジ3-1（図1）が、直接接続される場合の認証処理を説明する図である。

【0047】

まず、ブリッジ3-1の制御部35は、自分のCertificate、変数RelCntおよび変数AbsCntをソース1に送信する（図8①）。ここで、変数RelCntは、ブリッジ3-1が新たに得たい受信許可の台数を表わし、変数AbsCntは、既に得ている許可台数と今回許可を得たい台数の合計台数を表わしている。

【0048】

ソース1の制御部15は、これを受信すると、Certificateが正当なものか否かを、上述したDSA Verify演算処理を実行することにより判定する。そして、判定結果が、正当でない場合、認証処理は終了される。

【0049】

処理を継続する場合、ソース1の制御部15は、Certificate中の相手のIDが自分のIDリストに登録済みか否かを調べ、登録済みの場合、変数CntUpに変数RelCntを代入する。

【0050】

一方、IDリストにCertificate中の相手のIDが未登録の場合、ソース1の制御部15は、変数CntUpに変数AbsCntを代入する。そして、ソース1の制御部15は、変数SinkCntに変数CntUpを加えた値が、変数MaxSinkより小さいか否かを判定し、等しい場合、認証処理を終了する。

【0051】

そして、ソース1の制御部15は、擬似乱数Random_challengeを生成し、ブリッジ3-1に通信コマンドとして送信する（図8②）。

【0052】

ブリッジ3-1の制御部35は、この通信コマンドを受信すると、その値と送信済みの変数RelCntと変数AbsCntに対して、記憶部36に保持されている自分自身の秘密鍵を用いて、上述したDSA Sign演算処理を実行して、電子署名を計算する。ブリッジ3-1の制御部35は、計算された電子署名を、通信コマンド（Responseデータ）として、ソース1に送信する（図8③）。

【0053】

ソース1の制御部15は、この通信コマンドを受信すると、自分が送った擬似乱数Random_challenge、受信済みの変数RelCntおよび変数AbsCntに、この電子署名が対応しているか否か、すなわち、上述したDSA Verify演算処理を実行して、データの正当性を判定する。ただし、ここでは、先の鍵管理組織の公開鍵の代わりに、相手から受け取ったCertificate中の相手の公開鍵が用いられる。そして、判定結果が、正当でない場合、認証処理は終了される。

【0054】

処理を継続する場合、ソース1の制御部15は、コンテンツにかけた暗号を解くのに必要な鍵情報をブリッジ3-1に通信コマンドとして送信し（図8④）、変数SinkCntの値を変数CntUpの値だけ増加させた後、相手のIDがIDリストに未登録の場合、追加する。

【0055】

ブリッジ3-1は、鍵情報を受信し、それを使ってコンテンツにかけられた暗号を解いた後、再び暗号化してコンテンツを出力する。そして、ブリッジ3-1の制御部35は、変数MaxSinkの値を変数RelCntの値だけ増加する。

【0056】

以上の認証処理におけるブリッジ3の処理フローを図9に、またソース1の処理フローを図10に、それぞれ示す。

【0057】

また、図1に示されるソース1とシンク2-3、またはソース1とシンク2-4のように、ソース1より出力されたコンテンツが、2台以上のブリッジ3-1、3-2を経由した後に、シンク2-3、2-4に受信される場合、やはり、コンテンツを出力するブリッジ3-1（以下、Txブリッジと記載する）とそれを受け取るブリッジ3-2（以下、Rxブリッジと記載する）は、図8に示されたような認証処理を行う。

【0058】

なお、Rxブリッジの認証処理は、相手がソース1の場合と全く同じである。

【0059】

Txブリッジの認証処理は、図10のステップS46に示す処理が、ソース1の場合と異なる。具体的には、 $\text{SinkCnt} + \text{CntUp} > \text{MaxSink}$ の場合、Txブリッジは、変数MaxSinkの値を大きくするために、自分自身が入力しているコンテンツの発信元であるソース1またはブリッジ3に受信許可を要求する認証処理を行う（図1の例の場合、ブリッジ3-1はソース1に認証を要求する）。なお、この場合には $(\text{SinkCnt} + \text{CntUp}) - \text{MaxSink}$ 以上の受信台数の追加が要求される。この認証処理が成功した場合、図10のステップS50以降の処理が継続される。

【0060】

また、他の処理例としては、変数RelCntおよび変数AbsCntが、Certificateとは別に送信される場合が考えられる。例えば、図8③に示されたResponseと共に送信する方法、あるいは、全く別の通信コマンドで送信する方法もある。

【0061】

また、図7のステップS15、または、図10のステップS46において、ブリッジ3-1、3-2が、新たに接続されたソース1かブリッジ3と認証を行う場合、その結果によらず、その後の処理は継続しない方法もある。すなわち、新たな認証は、次回以降の認証を成功させるためのものと位置付けることができる。

【0062】

さらにまた、シンク2が自分の出力を受けるのを止め、暗号を解くのに必要な情報を失った場合、ソース1またはブリッジ3は、変数SinkCntをそのシンク2の分だけ減らすことができる。例えば、ソース1やブリッジ3がコンテンツにかける暗号の鍵情報を変更したら、シンク2は、自分自身の変数SinkCntを0にすることができる。

【0063】

以上のように、ソース1またはブリッジ3が、出力を受けられるシンク2の受信台数を制限するようにしたので、以下に示すような効果が得られる。

(1) コンテンツに関する権利者は、コンテンツの不正視聴や記録を未然に防ぐことができる。

(2) ブリッジを使って信号を再出力した場合でも、ソースは、ブリッジの先に

いるシンクも含め、台数を制限することができる。

(3) 台数の制限を機器固有のIDを使って行うことで、同じシンクが何度認証しても台数を誤って増やすことが無い。

(4) ブリッジが受信許可をソースや別のブリッジに要求する際に、受信台数の増加または減少分と受信合計台数を知らせることで、ソースや別のブリッジは、そのブリッジと認証したことがある場合、あるいは、認証したことがない場合のいずれにおいても、変数SinkCntを容易に、正しい値に変更することができる。

(5) 公開鍵暗号技術を用いることで、機器固有IDや要求台数を、安全に他の機器に渡すことができ、かつ、正しい台数管理を行うことができる。

【 0 0 6 4 】

上述した一連の処理は、ハードウェアにより実行させることもできるが、ソフトウェアにより実行させることもできる。一連の処理をソフトウェアにより実行させる場合には、そのソフトウェアを構成するプログラムが、専用のハードウェアに組み込まれているコンピュータ、または、各種のプログラムをインストールすることで、各種の機能を実行することが可能な、例えば汎用のパーソナルコンピュータなどに、記録媒体からインストールされる。

【 0 0 6 5 】

この記録媒体は、コンピュータとは別に、ユーザにプログラムを提供するために配布される、プログラムが記録されている磁気ディスク（フロッピディスクを含む）、光ディスク（CD-ROM(Compact Disk-Read Only Memory),DVD(Digital Versatile Disk)を含む）、光磁気ディスク（MD (Mini-Disk) を含む）、もしくは半導体メモリなどよりなるパッケージメディアにより構成されるだけでなく、コンピュータに予め組み込まれた状態でユーザに提供される、プログラムが記録されているROMやハードディスクなどで構成される。

【 0 0 6 6 】

なお、本明細書において、記録媒体に記録されるプログラムを記述するステップは、記載された順序に沿って時系列的に行われる処理はもちろん、必ずしも時系列的に処理されなくとも、並列的あるいは個別に実行される処理をも含むものである。

【 0 0 6 7 】

また、本明細書において、システムとは、複数の装置により構成される装置全体を表すものである。

【 0 0 6 8 】

【発明の効果】

以上のように、本発明の第 1 情報処理装置、第 1 の情報処理方法、および第 1 の記録媒体に記録されているプログラムによれば、コンテンツを暗号化し、他の装置より受信許可が要求された場合、他の装置と認証し、その認証結果に基づいて、コンテンツの暗号を解除する解除鍵とともに、受信台数を制限する制限情報を他の装置に送信するようにしたので、コンテンツの利用を制限することが可能になる。

【 0 0 6 9 】

また、本発明の第 1 情報処理装置、第 1 の情報処理方法、および第 1 の記録媒体に記録されているプログラムによれば、他の情報処理装置に対して、受信許可の要求を送信したとき、コンテンツの暗号を解除する解除鍵とともに受信台数を制限する制限情報を受信し、受信された解除鍵に基づいて、コンテンツを復号した後、暗号化する。そして、受信された制御情報に基づいて、暗号化されたコンテンツを他の装置に出力するようにしたので、コンテンツの利用を制限することが可能になる。

【図面の簡単な説明】

【図 1】

本発明を適用したネットワークシステムの構成例を示すブロック図である。

【図 2】

図 1 のソースの詳細な構成例を示すブロック図である。

【図 3】

図 1 のシンクの詳細な構成例を示すブロック図である。

【図 4】

図 1 のブリッジの詳細な構成例を示すブロック図である。

【図 5】

ソースまたはブリッジとシンクの認証処理を説明する図である。

【図 6】

シンクのソースまたはブリッジに対する認証処理を説明するフローチャートである。

【図 7】

ソースまたはブリッジのソースに対する認証処理を説明するフローチャートである。

【図 8】

ソースまたはTxブリッジのRxブリッジの認証処理を説明する図である。

【図 9】

RxブリッジのソースまたはTxブリッジに対する認証処理を説明するフローチャートである。

【図 1 0】

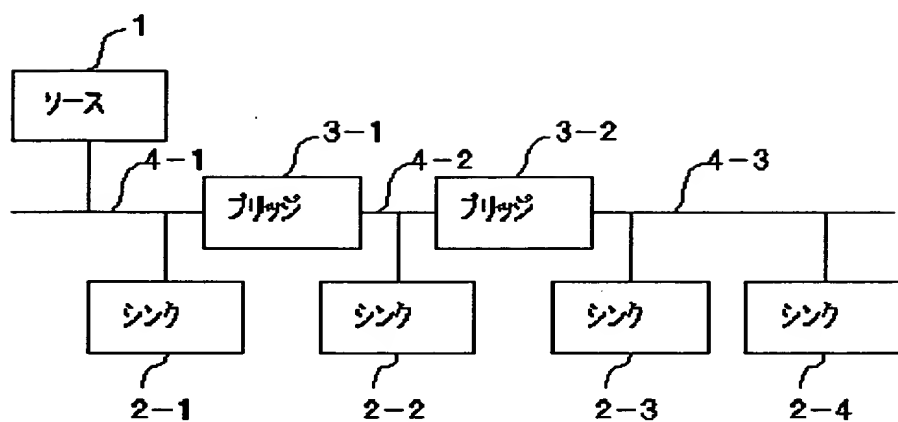
ソースまたはTxブリッジのRxブリッジに対する認証処理を説明するフローチャートである。

【符号の説明】

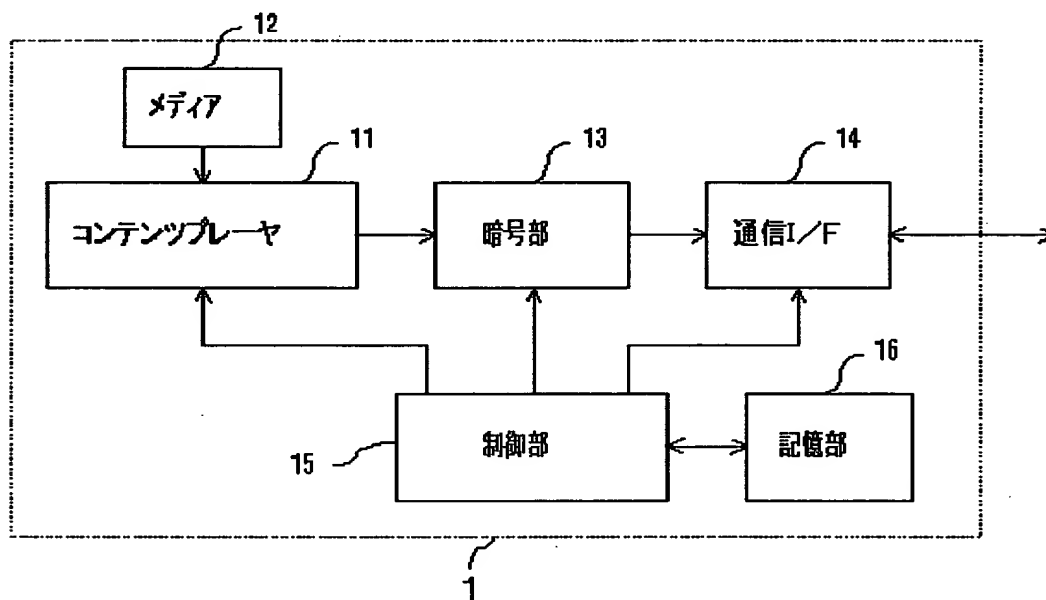
1 ソース, 2-1 乃至 2-4 シンク, 3-1, 3-2 ブリッジ, 1
1 コンテンツプレーヤ, 1 2 メディア, 1 3 暗号部, 1 4 通信 I/
F, 1 5 制御部, 1 6 記憶部, 2 1 画像・音声出力部, 2 2 復
号部, 2 3 通信 I/F, 2 4 制御部, 2 5 記憶部, 3 1 通信 I/F,
3 2 復号部, 3 3 暗号部, 3 4 通信 I/F, 3 5 制御部, 3 6
記憶部

【書類名】 図面

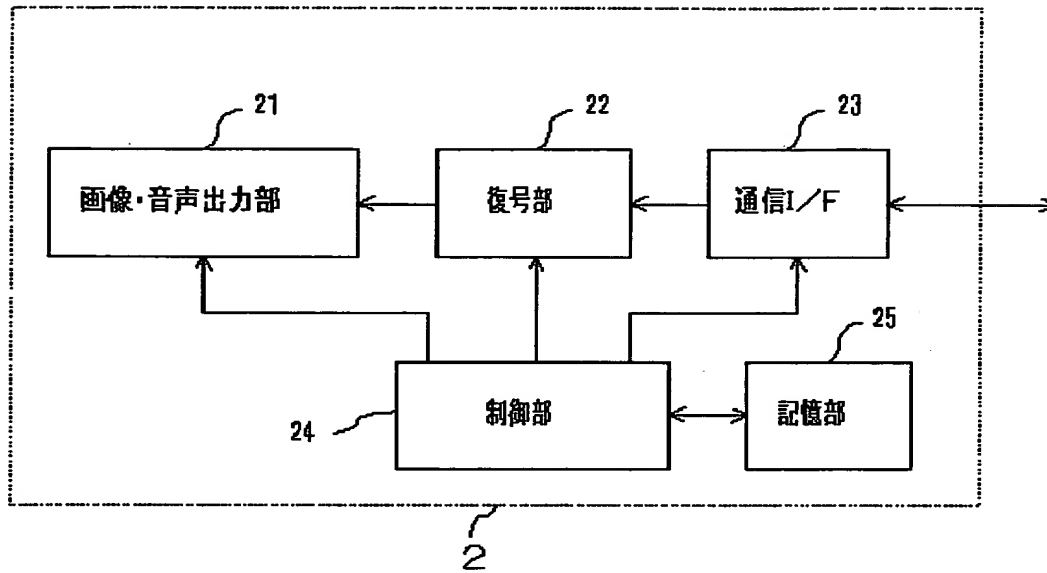
【図 1】



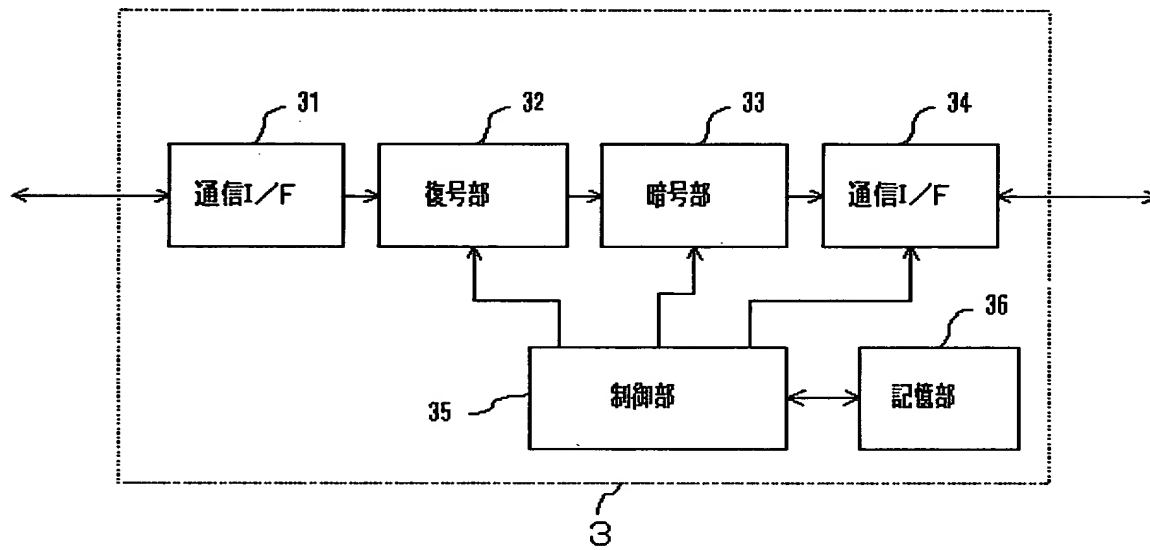
【図 2】



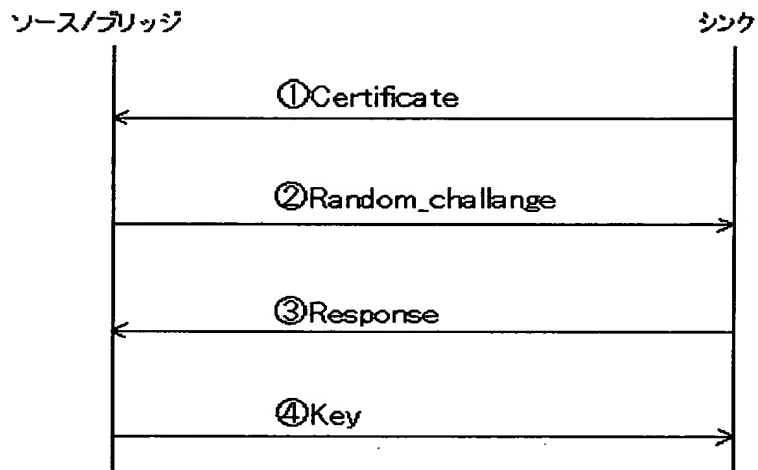
【図 3】



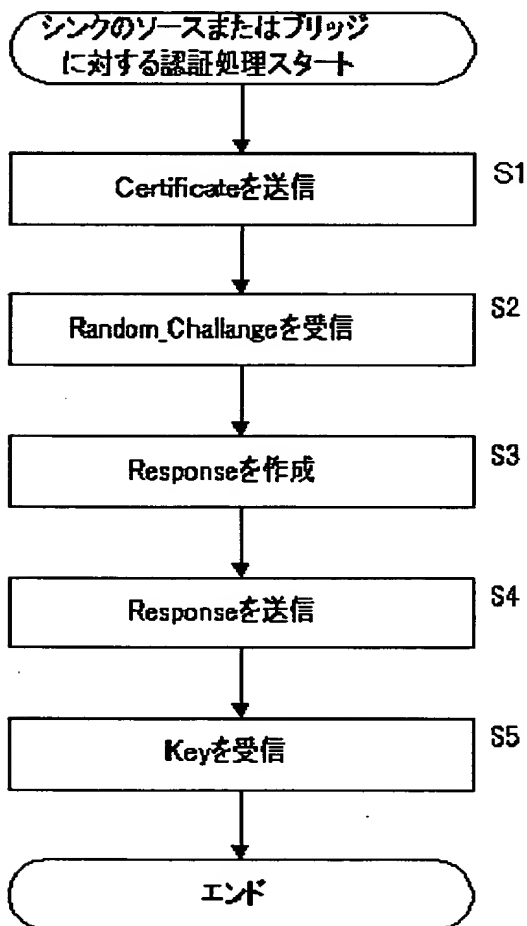
【図 4】



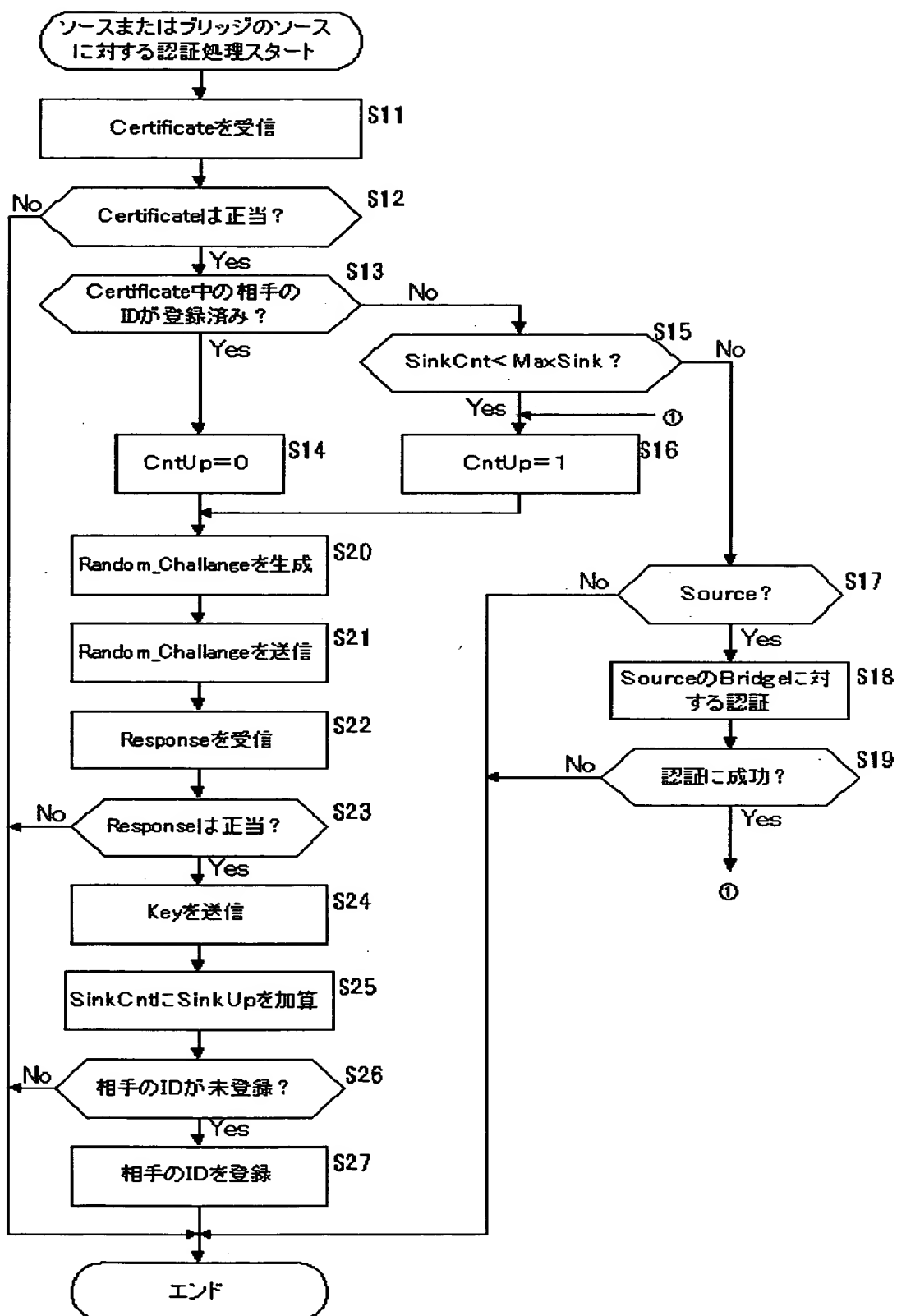
【図 5】



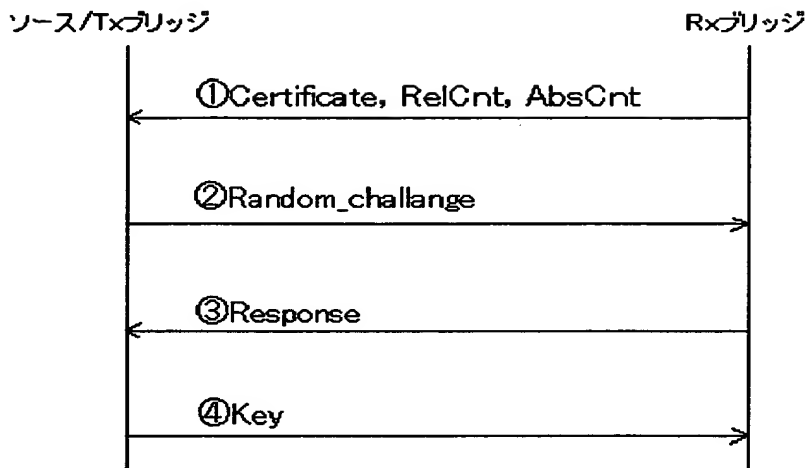
【図 6】



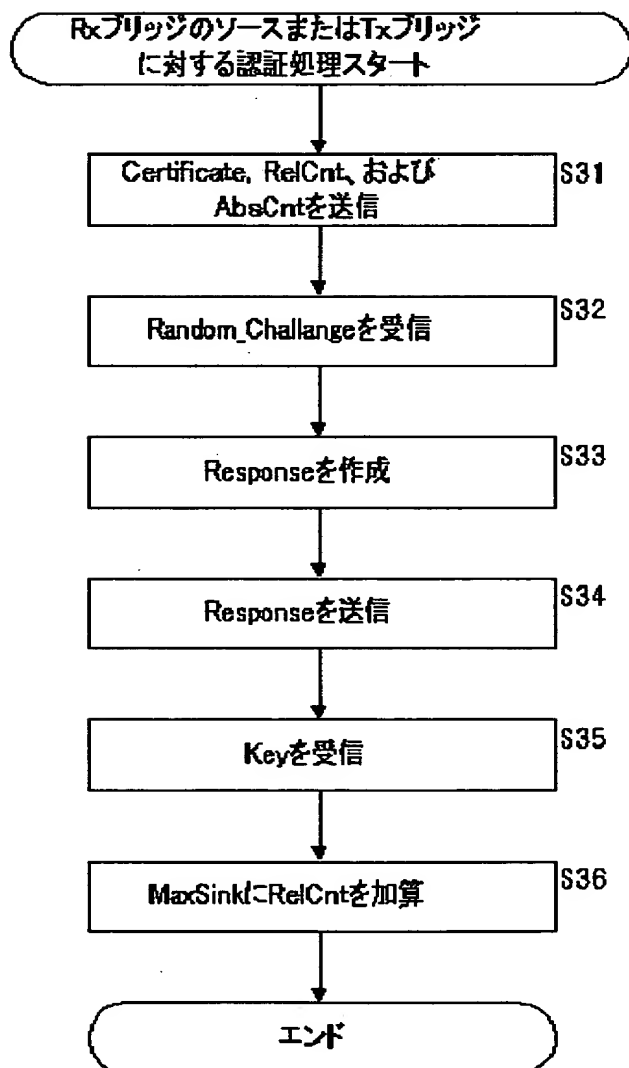
【图7】



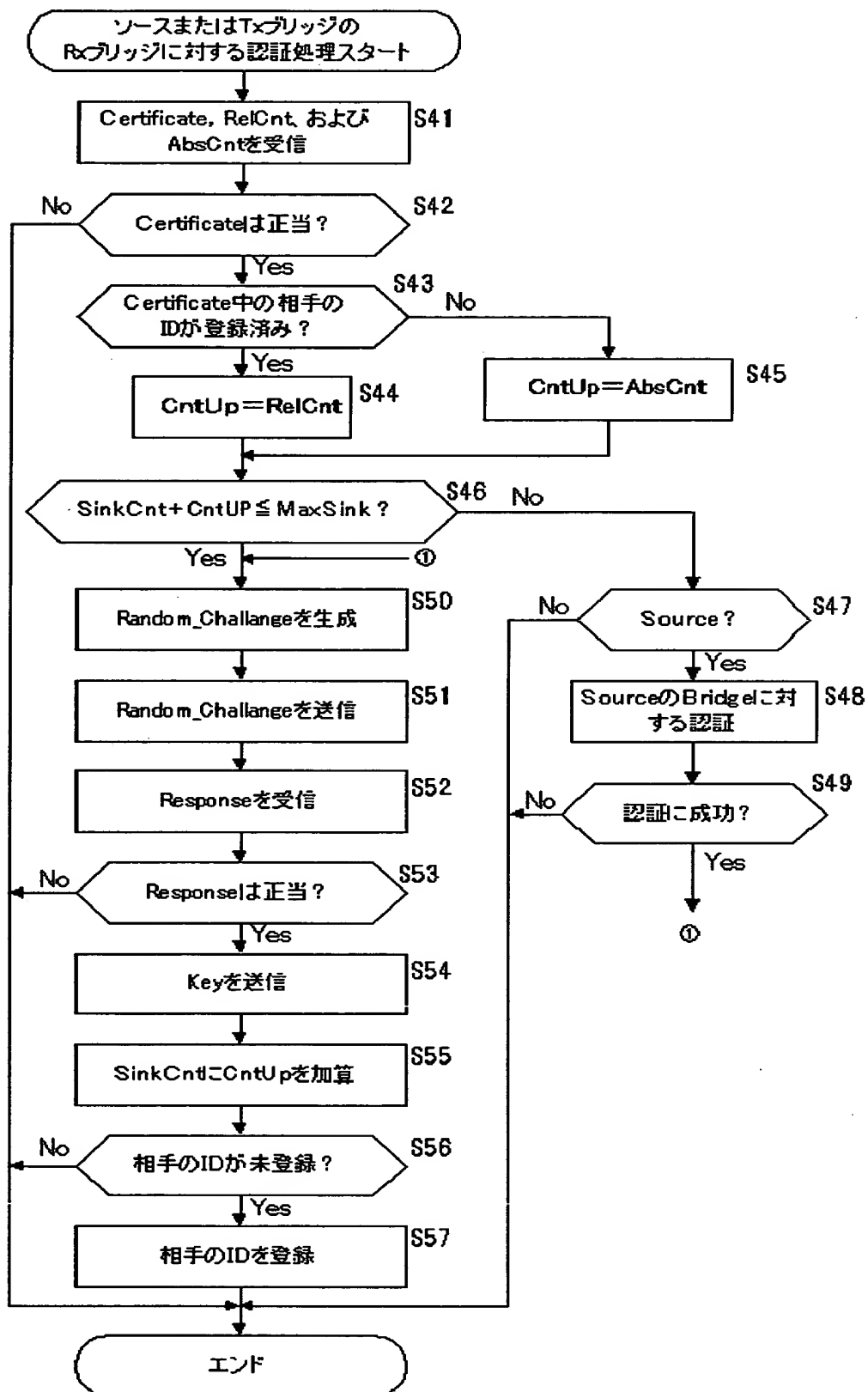
【図 8】



【図 9】



【図10】



【書類名】 要約書

【要約】

【課題】 コンテンツの利用を制限することができるようにする。

【解決手段】 ソース1は、シンク2-1よりコンテンツの送信要求を受けた場合、認証処理を行う。そして、認証に成功した場合、ソース1は、コンテンツにかけた暗号を解くのに必要な鍵情報をシンク2-1に送信する。シンク2-1は、鍵情報を受信し、それを使ってコンテンツにかけられた暗号を解くことにより、コンテンツを受信することができる。

【選択図】 図1

出 願 人 履 歴 情 報

識別番号 [000002185]

1. 変更年月日	1990年 8月30日
[変更理由]	新規登録
住 所	東京都品川区北品川6丁目7番35号
氏 名	ソニー株式会社